Forecasting Unknown/Unknowns by Boosting the Risk Radar within the Risk Intelligent Organisation

Alasdair Marshall

Southampton Business School, University of Southampton, UK

Udechukwu Ojiako

College of Engineering, University of Sharjah, UAE

Hull University Business School, University of Hull, UK

Victoria Wang

Institute of Criminal Justice Studies, University of Portsmouth, UK

Fenfang Lin

Southampton Business School, University of Southampton, UK

Maxwell Chipulu

Southampton Business School, University of Southampton, UK

Abstract

This theoretical perspective paper interprets *(un) known-(un) known* risk quadrants as formed from abstract and concrete risk knowledge. It presents these quadrants as useful, both for categorising risk forecasting challenges against levels of abstract and concrete risk knowledge typically available, and for psychometric research measuring perceived levels of abstract and concrete risk knowledge available for forecasting. Drawing on some cybersecurity risk examples, a case is made for refocusing risk management forecasting effort towards raising unknown-unknowns into known-knowns. We propose achieving this by

developing the ‘boosted risk radar’ as organisational practice where suitably ‘risk intelligent’ managers gather ‘risk intelligence information’, such that the ‘risk intelligent organisation’ can purposefully co-develop both abstract and concrete risk forecasting knowledge. We illustrate what this can entail in simple practice terms within organisations.

Key words: risk intelligence, competitive intelligence, military intelligence, risk radar.

1. Introduction

The present paper develops a theory of mature organisational risk management focused on risk forecasting knowledge production, where forecasting infrastructure converts ‘unknown-unknown’ to ‘known-known’ risk through more proactive effort to explore the organisational environment than is typically associated with the risk management function. To that end it advocates that organisational risk forecasting infrastructure be developed, *firstly,* through a novel theoretical approach to purposeful risk forecasting knowledge production, and *secondly,* as a more practical corollary, through terminological innovation: specifically the interrelated high-level guiding constructs of ‘risk intelligence’ and the ‘boosted risk radar’. Use of these, we argue, can focus practitioner aspirations towards greater awareness of how organisational risk forecasting knowledge can be developed and used effectively. Furthermore, we illustrate simple practical changes to risk related organisational processes and activities which can facilitate this.

Emphasising the need for more proactive investigation and interaction with threat sources as a means to gather the risk intelligence base for risk forecasting knowledge production, the paper engages critically with the dominant contemporary risk management paradigm which takes enterprise-wide risk management (ERM) (Committee of Sponsoring Organisations of the Treadway Commission, 2017) and strategic agility-oriented resilience

(British Standards Institution, 2014) as shaping how cutting-edge advances in risk management maturity are usually conceived. Generally speaking, we engage with this paradigm as follows. Theories of ERM and resilience both speak to the need for a ‘corporate nervous system’ for negotiating the corporate risk environment, to use the well-worn ecological and biological-adaptive metaphor (Institute of Risk Management, 2011). This metaphor’s various layers of meaning have been widely studied from Morgan's (2006) organisation-as-brain and organisation-as-organism perspectives. Furthermore its concern with interplay between corporate brain and corporate risk environment permits its wide use as convenient practitioner simplification for multiple overlapping 'open', 'organic' and 'cybernetic' systems theory perspectives within organisation theory (Scott, 2003) which draw upon diverse literatures to address this same interplay.

Following the convention of drawing eclectically from these literatures, we will argue that in today’s increasingly fast-moving, technology-driven and contingent organisational risk environment, risk management needs to be concerned with building corporate nervous systems, not primarily to drive strategy and agility *per se*, but more pressingly to ensure that organisational risk management forecasting effort engages much more proactively than hitherto with ‘unknown-unknown’ risk, to enable better and more rapid response. We recognise that a substantial literature on managing the unexpected through resilience, as illustrated by high reliability organisation practice (Weick and Sutcliffe, 2001; Weick and Putnam, 2006) is already deeply engaged with the broad challenge of facilitating early detection and rapid response towards ‘unknown-unknown’ risk (whose meaning we will shortly explore). Nonetheless we regard such literature as insufficiently concerned with proactive and targeted organisational effort to investigate and interact with possible threat sources in order to fill the risk knowledge vacuums that are fundamentally at issue, for both knowledge components that comprise every unknown-unknown risk.

In emphasising proactive knowledge-seeking as a foundation for risk forecasting, we conceive of knowledge accumulation as a socially distributed accomplishment grounded in complex everyday organisational practice (Orlikowski, 2002), such that we can theorise increasing levels of particular knowledge accomplishments in terms of the competences they produce for forecasting (especially complex) risks. Thus, we develop the metaphorical 'risk radar' concept, which we consider underused within its present theoretical positioning at the front end of the resilience process, through a novel focus on what it can mean to 'boost' it to reach out much further into the organisation's social threat environment. More fully, we extend the metaphor's meaning beyond passive detection of threat to further convey the need for targeted investigation and social interaction with sources of threat to obtain risk information and develop risk knowledge (which we further suggest should be structured using the knowledge categories we propose).

Our approach will also emphasise the insufficiency of compliance-driven and internal control focused risk management infrastructure whose centrepiece is the traditional risk listing process and its attendant risk registers. These practices too, we will argue, stand to benefit from enhancement through the 'boosted risk radar'; indeed we argue that the boosted risk radar's interface with the risk identification stage of the organisation's preferred risk management process should be of great interest to any organisation seeking risk management which is both more integrated and more capable of urgent response.

Our critical reflection upon the above 'traditional' risk management practice will emphasise opportunity for greater engagement with particular social threats posed by market competitors as well as all manner of corporate mal-wisher, perhaps most notably including cyber-hackers and others seeking to penetrate corporate security vulnerabilities. We will group these together as 'particular' social threats on the basis that they all entail reflexive human agency targeting particular organisations. Accordingly, what matters most for our

theory development purpose is that for particular social threats we can often theorise some dynamic and evolving attack-defend relationship concerned to either exploit or reduce some organisational vulnerability. In such threat contexts, we suggest, the need to convert 'unknown-unknown' risk by proactively seeking and engaging with the threat sources, has grown immensely.

The fundamental aim of this paper, then, is to work within the theoretical template outlined in the following section (which looks in detail at Rumsfeld's knowledge categories), in order to thereafter explore, both terminologically and in more practical terms, how organisations can dedicate forecasting effort towards converting unknown-unknowns into known-knowns. To support this, section 1.2 will extend the theoretical and literature context for the study.

2. (Un) known-(un) knowns

2.1 The four quadrants

Here we explain the origins of, and interpret the meaning and value of, the four *(un) known-(un) known* risk quadrants. In February 2002, US Secretary of Defense Donald Rumsfeld gave a media briefing which became widely referenced – within highly diverse academic literatures - for the terms it used to categorise military threats posed by Iraqi President Saddam Hussein's regime. Rumsfeld offered three categories: things we know we know (known-knowns), things we know we don't know (known-unknowns) and things we don't know we don't know (unknown-unknowns) (CNN, 2016).

To link this idea to relevant academic literature, in the first instance it appears that knowledge as competence-oriented social accomplishment (Orlikowski, 2002) is at issue. Longstanding academic literature dealing with this idea emphasises that knowledge is social and cultural (Nicolini et al., 2016) as well as dialogical (Tsoukas, 2009) in character.

Accordingly, we might view its level as slowly increasing within organisations, for particular risks; perhaps especially for complex risks whose causal understanding is highly multifactorial. Furthermore, we may differentiate such knowledge from the 'information' it stems from. It is often maintained that although information and knowledge are always about something (for our purpose, some forecasted risk), knowledge gathers and discerns patterns within information and can therefore be understood as contributing texture and sharpness to forecasts for complex risk. Insofar as such knowledge has its mettle tested by risk experience, we can begin to call it accumulated 'wisdom' (Rowley, 2007) and furthermore we can theorise and measure the value it creates (Smith and Raspin, 2011). The work by Smith and Raspin (2011) on organisational knowledge production illustrates how marketing literature in particular has developed a strong focus on knowledge development (Jaworski and Kohli, 1993) through its concern to cultivate marketing intelligence and thereafter create measurable value from any marketing ‘insights’ found. Such practice is in part rooted in resource-based theories of the firm (Barney, 1991), yet as we later explain in section 4, it also deeply reflects how businesses have learned from Rumsfeld’s domain: military intelligence.

Recognising that speculation on hostile weapons capability was clearly Rumsfeld’s focus during his 2002 briefing, it is plain that both the first and second knowledge components forming his (*(un) known-(un) known* were intended to take some risk as their object. It also seems reasonably certain that they were intended to denote separate categories of knowledge, which can be synthesised somehow to improve overall risk knowledge. Yet Rumsfeld was widely pilloried because the precise meaning of each knowledge component, and its relationship to the other, remained unexplained.

Prima facie, it might be speculated that the first knowledge component simply estimates uncertainty for the second knowledge component. Hence, for example, a known-unknown might express knowledge of high uncertainty for the destructiveness, readiness or

precise nature of a weapon. However, this begs the question of how the first knowledge component could ever be an unknown. Another possibility, more germane to the risk forecasting knowledge subject matter of our paper, is that while the second knowledge component always comprises forecasting knowledge pertaining directly to some possible weapons use event, the first component always adds the stamp of some knowledge enhancement, achieved through further critical reflection on the evidence base, method or theoretical frame employed to produce that forecasting knowledge. What makes this interpretation rather simplistic, however, is that *both* knowledge components can be viewed as corrigible through critical metacognition directed towards some theory, evidence or method used in its production. Recognising this, it could be argued that the difference arises through time ordering: the first knowledge component always takes the second as its object for critical metacognition irrespective of content. On that interpretation, Rumsfeld's *(un) known-(un) known* are useful for expressing the extent to which secondary layers of governance or lines of defence have been brought to bear in some organisational process of risk forecasting knowledge development.

However a problem with this 'time ordered' or 'governance' based interpretation is that it neglects the possibility that risk forecasting knowledge development can be 'pushed' in the reverse direction for various reasons, including those of socio-technical manipulation. For example, a known-unknown might comprise geopolitical-agenda-driven theoretical speculation about a weapons threat, which may in some cases serve as a 'false flag' pretext for initiating long planned military aggression. In such cases, the 'known' would comprise speculative, theoretical knowledge and the 'unknown' would refer to either the absence of evidential knowledge pertaining directly to the threat, or to the withholding of that knowledge from the public for security reasons. Hence, this could be a known-unknown from the public standpoint and a known-known for the military planners.

To more fully appreciate the value of theoretical inquiry into Rumsfeld's categories, which takes all of the above considerations into account, Pawson et al.'s (2011) study of how Rumsfeld's terms can inform realist theories of policy development is of interest. They call attention to the need for a 'steady conversion of unknowns to knowns' for both knowledge components. This, they say, entails not only cultivating an evidence base for scrutinising policy arrangements but also appreciating the complex nature of both theoretical speculation and evidence. Looking from this psychological realist standpoint, we might value Rumsfeld's categories as permitting the articulation of a particular psychological realist agenda: that of slowly and incrementally overcoming problems of human frailty in the conversion of unknown-unknowns into known-knowns, through a critical concern to explore (sometimes imbalanced) interaction between the two knowledge components at issue.

Logan (2009) offers a philosophy of science interpretation of Rumsfeld's categories, providing an excellent reason for valuing the first knowledge component for its often benign and constructive influences upon the second. He points out that scientific hypothesis testing in ideal situations is for 'known-unknowns'; that is, the theoretical knowledge comprising the hypothesis is known and the empirical findings, at least prior to the experiment' are unknown. In cases where findings lie out with the range of possibilities permitted by the theory, Logan (2009) argues, the thing under study should however be regarded as an '*unknown-unknown*'. This emphasis on the importance of theory testing to produce knowledge is notably consistent with all interpretations offered above.

A final enhancement to how we might interpret Rumsfeld's terms is offered by celebrity cultural critic Slavoj Zizek, whose critical commentary on the three binary categories raised the unmentioned fourth possibility: unknown-knowns (Zizekian Studies, 2015). Zizek's argument was that the second knowledge component can comprise ideological belief. Writing from a psychoanalytic perspective emphasising unconscious motivation, his

point was that it is possible to be motivated by an ideological worldview while lacking critical metacognitive awareness of how the resulting agency relates reflexively to its influence as a societal force. Zizek's view is, accordingly, useful for reminding us that risk knowledge production can only benefit from the focusing of critical metacognition towards culturally primed risk beliefs on multiple social levels.

Recognising that for all the above interpretations, there is value in exploring the interplay between the two knowledge components they theorise to exist, we contend that the best way to capture this value within an integrative theoretical simplification is as follows. Firstly, we reaffirm that both knowledge components can be viewed as referring to varying levels of socially distributed risk forecasting knowledge within organisations, improvable through critical awareness of how their interplay bears upon the overall production of risk forecasting knowledge. Secondly, we suggest that psychology literature dealing with the use of 'abstract' and 'concrete' mindsets to structure and develop knowledge holds the key to how we can differentiate these knowledge components in simplifying terms. Vallacher and Wegner (1985) contrast the more abstract and purpose-oriented 'why' of actions with the more process-oriented and concrete 'how' of actions to differentiate the separate emphases of these mindsets. Crutch et al. (2009) illustrate the complexity of this subject matter at the semantic level by studying how abstract and concrete words each relate to separate representational frameworks. Abstract words, they maintain, interrelate primarily through varying forms of mental association. This can produce useful simplifying and sometimes metaphorical understandings of complex reality. Concrete words, by contrast, interrelate more taxonomically to produce meaningful and ordered understanding of what is actually observed or observable.

Aiming for a more succinct differentiation pertaining more specifically to risk forecasting knowledge, we suggest that a more 'abstract' mindset for risk forecasting

knowledge can be understood as expressing theoretical imagination in terms of abstract categories and forms of risk, perhaps also linking abstract occurrences mechanistically (see Elster, 1989) to create narratives for risk events. This theoretical imagination might employ complexity-reducing metaphor or draw heavily on isomorphic learning to explain events as recurrences of previous similar ones. A more 'concrete' mindset, can be understood, by contrast, as data-driven and rooted in context-specific description. We can further characterise the abstract mindset in terms of risk imagination strongly influencing risk perception; the concrete mindset, by contrast, we can view as exerting influence in the reverse direction, with risk perception forming from actual risk experience and related data, in turn sometimes thereafter reshaping the broader abstract context of risk imagination. Accordingly, we theorise the two, in overview, as corresponding to forecasting knowledge shaped principally by explanatory risk imagination and by descriptive risk observation respectively. Notably, this simplifying interpretation entails that the former can include knowledge produced through moral imagination (Werhane, 1999) which might motivate risk forecasting effort to take the longer and larger view.

Our resulting 'abstract' and 'concrete' risk forecasting knowledge components give rise to the four quadrants below (figure 1):

Figure 1: Four States of Risk Forecasting Knowledge

Known Knowns *Risk is known both abstractly (in correspondence to events which do or may happen) and as a concrete risk exposure whose portents or impacts are described.*	**Unknown Knowns** *Risk is less well known abstractly but nonetheless individual or organisational experience of it necessitates its management.*
Known Unknowns *It is understood that a particular type or category of risk event demands attention yet there is an absence of evidence for its*	**Unknown Unknowns** *Possible risk events which have not been imagined/conceptualised and evidence for whose relevance within some specific*

presence as a concrete risk exposure for the organisation at issue.	*organisational context might exist embryonically as scattered information but not as coherent risk knowledge.*

Given that we theorise the risk forecasting challenge as one of raising knowledge levels from 'unknown-unknowns' to 'known-knowns', we suggest that the above four quadrants might be useful for expressing current estimated knowledge levels using psychometric mapping; that is, expert or practitioner estimates could be displayed for expert and concrete knowledge levels in relation to specific forecasting challenges.

We further propose that in order to raise knowledge levels from unknown-unknown to known-known status it is helpful to consider the following four points. Firstly, traditional risk management deals in known-knowns insofar as its subject matter is (often insurable) regularly occurring risk events. These are ideal risk conditions for ongoing refinement of high levels of abstract and concrete risk forecasting knowledge. Secondly, known-unknown risk events may often be planned-for events, where planning protocols are created, tested and improved using red-teaming and other forms of scenario exercise. Moreover, the term is useful for highlighting possible management-of-uncertainty challenges should such events occur. For example, the World Health Organisation has recently proposed that scientists and public health emergency planners prepare for the 'known-unknown pathogen' they call 'Disease X' (Nuki & Shaikh, 2018). Their point, in using Rumsfeld's binary category, is to emphasise the practical necessity of making preparations for a fast-spreading global epidemic which will place managers in knowledge poor circumstances. Thirdly, we can view unknown-known risk forecasting challenges as sometimes characterised by the presence of knowledge of 'what' is happening or might happen, in the absence of knowledge pertaining to 'why' it is happening or might happen. Following Zizek's theoretical approach, we might look to examples characterised by difficulties in understanding behaviours, either because plausible psychological explanations are contestable and/or they invite interpretive bias. Unknown-

knowns, then, are perhaps best understood as relating to unfolding events which clearly matter, but where explanatory theoretical context is highly problematic, perhaps often - but not necessarily – because their human aspects are hard to interpret without ongoing doubt and controversy. Finally, we suggest that it may be possible to become more sensitised to the risk forecasting challenge of converting 'unknown-unknowns' into 'known knowns' by exploring whether the above known-unknown and unknown-known problems constitute the most pressing obstacles.

Before setting out our suggestions regarding how organisations can engage with this conversion challenge, we must however look at unknown-unknowns in more detail. Our approach is to recognise their growing salience within today's security climate; wherein low probability-high impact 'Black Swan' events, especially cyber security related events, proliferate. The past decade has presented a never-ending stream of cyber 'Black Swan' events, affecting governments, businesses, and the general public. Some of the higher profile ones affecting nation-states include the Stuxnet attack in 2010 (Langer, 2011), the Red October botnet attack (2012) (Vikos and Gritzalis, 2013), the Mask malware attack (2014) (Kaspersky, 2014), and the recent WannaCry ransomware attack (2017) (Sahi, 2017). More recently and relevantly, there has been a series of 'particular' social threats in terms of targeted data breaches, affecting large organisations, such as Uber (2017), Equifax (2017), and Deloitte (2017). Looking ahead to the future, we can expect the scale, severity and complexity of targeted cyber 'Black Swan' events to continue to increase. Yet, we still lack sufficient theoretical and practical means to direct forecasting effort towards these events that we call 'unknown-unknowns'.

2.2 Application of the Theoretical Template: objectives and literature context

In the remaining sections of this paper, the common thread will be our advocacy for the use of new and adapted risk management terminology to allow organisational risk management to better convert 'unknown-unknown' risk forecasting knowledge and, at the same time, greatly enhance risk forecasting knowledge for corporate cybersecurity and other particular social threats. Our two objectives will be to: (i) develop key concepts for exploring how organisations may proactively detect and defend against particular social threats from individuals or other organisations; and (ii) explore implications for the nature and scope of risk management practice, seeking in particular practical ways of co-developing abstract and concrete risk forecasting knowledge. First we meet objective one through critical discussion of our new 'boosted risk radar' concept, which is essentially a high level abstract metaphor. Secondly we meet objective two through critical discussion of our proposed multi-layered 'risk intelligence' concept which engages on more practical levels with how organisational risk management can pivot towards forecasting for unknown-unknowns and related knowledge conversion concerns.

Our particular concern with raising risk forecasting knowledge from unknown-unknown levels leads us to be especially interested in low probability-high impact threats. Lindaas and Pettersen (2016) consider these a key problem for the profession, exploring it like many others through the lens of how risk management might get smarter at handling 'black swan' events. Our proposals seek to contribute to this debate. Furthermore, we argue drawing from earlier work on unconventional and irregular social threat (Marshall et al., 2012; Chipulu et al., 2016), indeed including threats arising with market competition (see Ojiako et al., 2010), that remedies to particular social threats can usefully learn from how the military deals with asymmetric or unconventional warfare. This entails considering, for example, that information asymmetries as well as disparities in ethics and resources can be important when theorising circumstances of, and relationships between, attackers and defenders. We have

already touched upon why critical attention to relative levels of abstract and concrete risk knowledge can be vital for understanding conflict.

A review of related literature suggests that particular social threats may be characterised by ongoing reflexivity in attacker-defender relationships. Drivers of attack persistence and reinvention over time might often include perceived social (Donnelly-Saalfield, 2009; Ifedi and Anyu, 2011), ethical (Schminke et al., 2014; Chipulu et al., 2016) or service (Grégoire and Fisher, 2008; Grégoire et al., 2009; Fisk et al., 2010; Daunt and Harris, 2012) violations by the targeted firm. We further contend that it is important to understand how organisations which normally compete 'within the rules' are likely to effectively recognise, monitor and manage threat actions that are purposeful, targeted and sometimes episodically repeating, yet hard to predict because the agencies are anonymous and prepared to violate laws and other norms. We recognise from learning-from-the-military literature (Ojiako et al., 2010, 2012; Marshall, 2012), that current risk management capabilities are underprepared for unconventional threats and competitive behaviours that subvert well recognised conventions. Also of interest within that context is Chen and Miller's (1994) suggestion that even reputable firms may engage in targeted threat actions when they deem the targeted firms major obstacles to their survival.

Organisational responses to particular threat actions appear under-studied within risk research literature. Such literature does exist in the management and marketing fields (see Chen and Miller, 1994; Grégoire and Fisher, 2008; Grégoire et al., 2009; Zourrig et al., 2009; Ojiako et al., 2010; Nepomuceno et al., 2017). In risk management literature all such concern is eclipsed by what is seen as a greater concern to develop faster and better responses to all sorts of threat. Accordingly numerous scholars such as Power (2004, 2009), Ojiako et al. (2010), Marshall and Ojiako (2013, 2015, 2018, 2019), Wu et al. (2014), Huang et al. (2016), Leva et al. (2017), Slonim (2017) and Smyth (2017) have concerned themselves with

developing broader and more holistic risk management approaches than those which have focused historically on narrow risk management processes that match anticipated risks to controls. This has arguably led over time to a blending between the risk-based internal control, enterprise risk management, resilience, crisis management, business continuity and organisational agility concepts which we outlined earlier. Ambitious risk management approaches of this nature sometimes call on 'risk radar' concepts (Jovanovic, 2012; Jovanovic et al., 2012; Huang et al., 2016) to denote environmental scanning. Central to this metaphor is the idea that proactive scanning is involved (radar equipment must transmit before it can detect anything) and further important denotations of meaning are that radar can be intelligently located and directed. In the first half of this paper we further develop the metaphor by conceiving of the risk radar as something that can be 'boosted' to generate abstract and concrete forecasting knowledge for particular social threat. Acknowledging that the test for a good organisational metaphor is whether it can inspire collaborative creative thinking within organisations (Biscaro and Comacchio, 2017), we argue that our boosted risk radar metaphor might help guide the further development of the risk management profession.

3.0 Early warning risk radars

3.1 Ownership of the risk radar

When conceptualised in its broadest scope as a risk assessment information gathering and processing system (Jovanovic, 2012; et al., 2012; and Balos, 2013; Huang et al., 2016), the objective of the *'risk radar'* is to facilitate the recognition, monitoring and management of risk. Working within the metaphor, this entails locating risk and communicating findings to relevant parties. Clearly, both the theoretical imagination of the abstract mindset, as well as the concrete mindset's concern to interrogate and be led by data, are both vital considerations. For broad organisational context, we can situate the risk radar within the context of

Enterprise risk management (ERM) approaches which align the management of risks to governance structures, strategy, and more recently performance (Aven and Aven, 2015; Bromiley et al., 2015, COSO, 2017). However, the main theoretical offering of this paper is to explore how the risk radar can gather, process and communicate intelligence to create the risk intelligent organisation. Here, the risk intelligent organisation is an organisation with capabilities to not only support effective early warning about enterprise risk in general, but also to counter irregular, audacious and non-routine threats, engagement or competition from individuals or organisations. We also view such risk intelligence as corrigible in part through critical overview of what abstract and concrete risk forecasting knowledge is available.

According to Ansoff (1975, p. 22), in response to 'weak signals', organisations generally can choose to be reactive or proactive. If they choose to be reactive, it involves developing competencies for quick and efficient crisis management. Alternatively, if they choose to be proactive, it implies having in place effective means of scanning and then actively interrogating whatever is found to be of interest within the environment (Hambrick, 1981; Elenkov, 1997; Crant, 2000; Parker et al., 2010). Our paper can be viewed as extending this literature through its exploration of the interface between risk management and competitive intelligence functions, employing the term 'risk intelligence' partly to refer to their fusion. This creates a risk radar ownership issue. While a strong case can be made that risk radars are best championed and owned by the risk management function, the reality is that for effectiveness, the development of the risk radar will require firstly, systematic and constantly organisational-wide learning that supports the development and alignment of internal competencies linked by an expanded risk philosophy (Thompson, 1986; Valverde, 1991; Althaus, 2005; Campbell, 2006; Schiller and Prpich, 2014). Secondly, it will require the coordinated participation of various organisational functions (Braunscheidel and Suresh, 2009) including competitive intelligence. Such participation, we will argue, is best supported

by effort to encourage the participating functions to think beyond narrow departmental concerns. Some baseline level of participation by many or even all organisational functions may be desirable (see Balogun et al., 2005; Hoyt and Liebenberg, 2011). Our justification is that without such boundary spanning involvement the result may be risk radar coverage that reflects pre-existing organisational biases. A related possibility is that the resulting risk intelligence may not be communicated in a timely and coordinated manner; furthermore if insufficiently aggregated for various purposes, one consequence may be information overload at higher echelons (Foss and Rodgers, 2011).

Conceptualising the *'risk radar'* as an effective form of early warning invites further reflection on two key points. *Firstly*, risk management processes invite complex, fluid, or hybridised integration with various other management and governance processes within organisations (Lidskog and Sjödin, 2016). The broad challenge here is essentially one of information and knowledge management (Hoyt and Liebenberg, 2011), which in the context of our study is re-envisioned to accommodate the risk radar metaphor as the basic sensory apparatus through which the organisation becomes aware of and responds to particular social threat action. *Secondly*, conceptual awkwardness inevitably arises with the notion of a risk radar designed to receive and relay risk information while also performing a broader information gathering and processing role. For the organisation, what would matter is that *proactive* risk identification develops forecasting knowledge for threat action, particularly to enable fast response (Huurne and Gutteling, 2008), and furthermore that all gathered information or knowledge is also circulated throughout relevant organisational lattices with the speed and sensitivity it requires, as indeed has long been associated with enterprise risk management practice (Dickinson, 2001). Some literature (e.g. Thompson and Bloom, 2000; Lin et al., 2017) suggests that risk managers prefer risk information formatted for use within varying operational and strategic decision contexts, and for stakeholder circulation. Concern

with these broader contexts, Árvai (2014) argues, goes a long way towards ensuring that disconnections between how risks are defined, and how risk management is actually practiced, are reduced. Accordingly, we contend that it is particularly important to guard against any use of unnecessarily restrictive terminology or formatting whose effect might be to communicate risk information too narrowly and prevent its meaningful understanding as applicable knowledge (Huurne and Gutteling, 2008; Árvai, 2014; Lin et al., 2017).

3.2 Information gathering from a risk perspective

It follows from the above that the risk radar needs to look beyond what the lens of 'risk' renders visible. Accordingly we view it as a metaphor for coordinated attentiveness to the organisational threat environment, especially helpful for sensitising organisations to particular social threats which may affect organisational functions in different ways. Everything which risk radars do in this respect can be considered to involve matching risks to controls (Spira and Page, 2003). Arguably, organisational radars are always 'risk radars' because they focus purposefully towards risk-control matching in this broadest sense. In recognition of the fact that an astute grasp of both the past and the future requires agile use of both threat and opportunity frames to produce causal understanding (Sitkin and Pablo, 1992; Power et al., 2009; Aven and Aven, 2015), we also contend that effective use of risk radars may sometimes hinge on careful attention to these complex issues when developing knowledge (both abstract-mechanistic and concrete-sequential) pertaining to causal complexity within the social threat environment.

Perhaps the biggest problem with the risk radar concept arises where organisations simplistically regard it as a means to identify 'the risks' before these are conveyed through risk management processes for recording in risk registers and internal control systems. Perhaps we get close to the root of many flawed understandings of organisational risk

management (Hansson, 2004; Moosa, 2007), when we consider that such commonplace risk ideation might misattribute motional properties to risks. This entails the flawed imagining of risks as 'things' that move, that are then capable of 'impacting' on the organisation, yet which can also be transferred into various stages of the risk management process only to be 'caught' or 'captured' within risk registers and internal control systems. This confused metaphorical imagination of 'risk as motion' constitutes a category error in logic, because risks are not movable 'things'. Arguably, much more attention should be paid to the harm this flawed view of risk can cause. Our theory development will take some interest in this issue, as we do not wish to see the risk radar concept employed to perpetuate or even deepen such misunderstanding. Every metaphor has its limits (Cornelissen, 2005), and one limit of our risk radar metaphor is that by speaking to the commonplace metaphorical ideation of risks as moving objects, it invites all the attendant misunderstandings, not least of which is the problem of de-contextualising risks as discrete objects to be managed separately. We, by contrast, emphasise its role in enabling the production of risk forecasting knowledge over perhaps long time periods, with much less complexity reduction than simple risk-control matching entails.

3.3 Generating Marketing insights

The notion that risk radars may serve a more diverse range of organisational purposes leads to the proposition that they offer informational sources of competitive advantage classable as Consumer or other Marketing insights. Notably Smith and Raspin (2011) discuss organisational processes of knowledge development to produce consumer insight along these lines. A very relevant source for further opening out the risk radar concept, their work emphasises the need for elaborately designed scanning systems. Built into such systems are mechanisms which allow for not only the allocation of monitoring tasks to managers with

diverse competencies, but also alignment of such competencies with changing complexity and volatility levels in competitive environments. More specifically, Smith and Raspin (ibid.) characterise the rare moments of insight that scanning should aspire to create, in terms of four basic 'VRIO' criteria. These are that insights should: (i) offer 'value' for organisations, (ii) be 'rare' in the sense that competitors are unlikely to find them, (iii) not be 'imitable', in effect, competitors should lack capabilities to either find them or act upon them, and (iv) be aligned to 'organisational capabilities'.

We might even define the term 'risk insight' by these same criteria. Taking this view, the best practice suggestion arises that perhaps risk assessment processes would benefit from giving routine consideration to whether the risks under their purview might be handled differently when recognised as offering risk insight value. Routine quantitative scoring for the insight value of identified risks might even help to transform the value of risk registers as decision-making tools (a role whose importance has been emphasised in the literature – see Ackermann et al., 2007). This suggestion recognises that strategic decision-makers are more likely to value risk information which is communicated in ways that are consistent, unambiguous and easily understandable (Månsson et al., 2017). Yet this also problematizes the question of whether risk registers can and should be transparent. These can be considered key questions for our proposed risk radar use. However, the more general and key conclusion arising from this introductory discussion is that risk radars need to feed 'multilingual' communication and dialogue within organisations (see Ackermann et al., 2007).

3.4 'Boosting' the risk radar

Where particular social threat is at issue, urgent response capability becomes an important fitness-for-purpose test for risk radar infrastructure; however so too is the strength and reach of the radar signal that scans the social threat environment. Use of the risk radar may entail

not just information gathering close to primary threat sources, but conceivably also various forms of direct (remote-electronic or interpersonal) engagement and interaction. Accordingly we propose a notion of *'booster infrastructure'* centring on intense proactive engagement and interaction, perhaps sometimes with individuals or groups who harbour malice or competitive ill-will towards the organisation. This raises various skills, resources, law and ethics issues, several of which we consider below. We might even theorise such *'booster infrastructure'* as the key missing link within risk management thinking today. However, to reiterate strongly, any such enhanced risk management function would need to relax any semantic grip its favoured risk discourses, documentation and related visual representations might hitherto have either deliberately or unwittingly imposed on organisational information flows. In so doing, it should be better able to elicit enthusiastic participation in the organisationally distributed co-development of risk forecasting knowledge. In particular, it might be argued that risk management ownership of booster infrastructure should resist any temptation to process information through the conceptual straitjacket which Ackermann et al. (2007) associate with risk register use. A viable alternative may involve use of 'action point registers' which triage incoming information towards where it can most productively be assembled as forecasting knowledge (or business insight) with such urgency and confidentiality as are deemed appropriate.

3.5 A dangerous high stakes activity?

Critics of the above proposal may claim that active investigation of primary sources of risk information is best left to the area of fuzzy overlap between the competitive intelligence, business intelligence and marketing intelligence functions which already have well-established competency in this area (Freeman, 1999; Wright and Calof, 2006; Calof and Wright, 2008; Smith and Lindsay, 2012). Nonetheless, we suggest risk management can take

a leadership and coordination role, linking these functions to the rest of the organisation through a guiding theoretical concern with the purposeful cross-functional co-development of risk forecasting knowledge. As articulated in literature exploring the relationship between professions and institutional change (Daudigeos, 2013; Muzio et al., 2013), professions are able to utilise their expertise and legitimacy to initiate institutional pressures which bring new adjustments and changes, sometimes leveraged through the development new guides, standards and associated job descriptions. This has recently been the case with the rise of the 'Chief Risk Officer' role as a means to ensure enterprise risk management is taken seriously at the top management table (Aabo et al., 2005; Harrison and Phillips, 2014; Pernell et al., 2017; Karanja and Rosso, 2017). Correspondingly, we envisage risk management ownership of 'booster infrastructure' for risk radar as requiring new leadership and coordination roles, as well as related job descriptions and other forms of guidance.

4.0 ERM context for boosted risk radars

Speaking further to the above issue of cross-functional leadership and coordination, it can also be argued (see Aabo et al., 2005; Harrison and Phillips, 2014; Pernell et al., 2017; Karanja and Rosso, 2017), that the risk profession is *already* strongly aspirant towards subsuming various other - sometimes competing - organisational functions to serve its master concept of a singular, overarching, early warning risk radar for organisations. Such empire-building efforts by risk management entail that organisational groundwork for our proposal is already well established in many organisations. Thinking from the perspective of 'boundary maintenance' which explores how professions take shape and gain influence (Montgomery and Oliver, 2007, p. 665), the risk profession is fundamentally concerned to promote cross-functional information flows leading to knowledge development, because without them both ERM practice and resilience are impossible. Focussing on the theme of urgent response

which has come to matter greatly within both contexts of practice, the next section now looks more closely at how the risk radar concept has emerged to prominence within the context of resilience in particular.

4.1 Resilience context

The 'risk radar' is often considered a foundational principle of organisational resilience. The well-known *'Roads to Resilience'* (Franken et al., 2014) report recognises five such principles (the 5 Rs) as follows: (i) Risk radar should anticipate problems before they escalate, (ii) Resources and assets should be diversified, (iii) Relationships and networks should allow risk information to flow, (iv) Rapid responses should initiate before crises or disasters happen, and (v) Review and adaptation should occur *ex post.*

One important question, however, is whether the human alertness and proactivity constitutive of the risk radar should be limited by the boundaries of the organisation. Our contention that it should lay stronger emphasis on the need for managers with highly astute people skills to go out and actively explore the social world (thereby 'boosting' the radar) should be of interest in view of the risk profession's growing attention to third party risk and partnership risk (PWC, 2013). We live in an *'age of access'* (Rifkin, 2001) characterised by complex supply chains and fluidity in co-working and partnering between organisations. This entails that trust building and various inter-organisational challenges relating to security are growing in importance. Many new opportunities for malice towards organisations target the interfaces between organisations (Korsgaard et al., 2015) because this is where blind spots in risk radars are often to be found. We posit that this places an especially high premium on robust people skills where a specific concern with stakeholder relationship maintenance combines with a more general willingness to go out into the social world, in order to operate fit-for-purpose risk radars today.

4.2 Challenges

However there remain important further grounds for resisting the central proposal of this paper. Schoemaker et al. (2013) associate the production of knowledge through use of 'strategic radars' by (by networked firms in particular) with the particular problem of how to manage the data avalanche that can arise. Indeed their focus on forecasting for fast-changing technological risk, using scenario analyses activities, which bring stakeholders together, is of interest in the present paper insofar as our interest in cybersecurity risk places technological risk and related management approaches within the broader context of social threat and ongoing (cyber) attack-defence relationships. Such complex risks and the information aggregation challenges they bring can become more manageable by using 'red teaming' simulations in particular.

Another problem is that primary threat sources will be highly cautious in terms of disclosing any usable information concerning threats, which they themselves pose. They may take strong measures to prevent or dissimulate any such disclosure. On the one hand, the information-gathering challenges arising under these circumstances bolster our argument for critical juxtaposition of abstract and concrete risk knowledge, as a means to contextualise any information gleaned. Yet we still need to acknowledge that the closer an early warning risk radar gets to the source of a social threat, the more practical and ethical challenges it is likely to encounter. Hence, there may be points of diminishing returns and increasing risk from greater resource expenditures on boosting risk radars.

For a better understanding of such risk we could look from sociological and psychological perspectives of 'organisational edgework' (Lyng, 2005; Zinn, 2017). This entails considers information gathering encounters which push towards the 'edges' of appropriate behaviour as experiences characterised by intoxicating exhilaration, anxiety,

relief, reward etc. Although these edges will inevitably be circumscribed by law and other social norms, the edgework actually undertaken may often include at least *some* transgressive boundary work driven by the desire for such experience. An issue arising with information-gathering edgework, then, is whether negative financial and reputational impacts arising with either real or perceived transgression might sometimes outweigh anticipated benefits from information gained. The more a risk radar is 'boosted' as we propose, the more serious these issues of risk-adjusted return are likely to become. As we emphasise later on, professionalism in the application of relevant ethics codes can help address this problem. This can be facilitated, we will argue, through participation of the competitive intelligence profession in the riskier and more controversial aspects of risk radar use.

5.0 Risk intelligence: Three meanings

Having outlined some key organisational challenges and obstacles linked to our boosted risk radar proposal, we now engage more closely with its forecasting knowledge development concerns with reference to what we consider important facilitating terminology. In proposing three possible meanings of 'risk intelligence' which we think combine to provide the necessary terminological foundation for developing boosted risk radars, we are able to look at the challenges and obstacles on more practical organisational levels and recommend practical improvements within organisations.

5.1 Meaning One: Risk intelligence is managing risk *intelligently*

The first part of our paper established our concern with critical juxtaposition of abstract and concrete risk forecasting knowledge. We looked at possible advantages of this binary knowledge ontology, particularly as a stimulus for critical reflection. We further theorised purposeful conversion of such knowledge, moving from unknown-unknowns to known-

knowns. Moreover we viewed this as practice which can be initiated (and progressed in cases of persistent attacker-defender interaction) through 'boosted risk radar activity', bringing forward early detection of social threat through more purposeful interaction with its likely sources and those close to them. In this section, we now theorise 'risk intelligence' as offering further valuable risk management terminology which can help shape such practice. In particular, our view of 'risk intelligence' will, in this present section, be concerned with the intellectual, ethical and psychological wherewithal for gathering and developing risk forecasting knowledge for social threat.

Evan's (2012) theory of risk intelligence (RQ) concerns simple estimates (a subject matter substantially removed from forecasting for complex risks). While described generally as "a special kind of intelligence for thinking about risk and uncertainty" (p. 288), its more precise measurement focus is on resistance to false certainty when estimating probabilities for the correctness of truth claims. Similarly, several scholars focus narrowly on measurable aptitudes for thinking in rational (Stanovich, 2009a) or flexible (Mellers et al., 2015) ways about decisions under uncertainty. It is widely acknowledged (Frey and Detterman, 2004; Stanovich, 2009b; Stanovich and West, 2009), that such scientific approaches to measuring various forms of intelligence can however sacrifice valuable bandwidth in their quest for measurability. Correspondingly, we suggest that risk intelligence is most likely to become a useful psychological concept for risk practitioners when used openly and flexibly; furthermore it might be used most effectively where practitioners are encouraged to focus its range of psychological meanings towards what matters most for them, so that these meanings become captured for organisational learning purposes.

The human challenge in operating the boosted risk radar arguably lends itself to the following broad psychological view of risk intelligence, which might conceivably be promoted in organisations intent on boosting risk radar practice. Opening out some parallels

with the RQ construct, we can consider how risk radars will benefit from high IQ in particular ways. Consider for example the importance of cognitive problem-solving skills fundamental to IQ such as such as pattern recognition (Gottfredson, 1997). High competency in this particular skill might often be vital for flexibly balancing concrete risk knowledge with abstract explanatory and historical contextual knowledge, both for purposes of initial attunement towards social threat and for ongoing refinement of related forecasting knowledge (pertaining for example to changing intentions, plans or capabilities underlying such threat). We could also expand our scope to consider emotional intelligence quotient (EQ) (Salovey et al., 2004). High EQ's contribution to risk intelligence might include the insight it can bring to problems such as selective inattention to concrete risk information, which does not fit with affect-laden organisational narratives. It might even offer protective or curative benefit for problems of organisational paranoia (Kramer, 2008) which are bound to sometimes shape and weight prevailing risk forecasts for social threats. Turning to consider cultural intelligence quotient (CQ) (Brislin et al., 2006), we might also contemplate the risk profession's rapidly growing interest in cultural contexts likely to advantage or disadvantage accurate risk forecasting. Such intelligence may prove important for appreciating why abstract subtleties of cultural context (e.g. for hacker communities) can matter when theorising social threats to organisations. Taking stock, then, we might usefully view risk intelligence as a composite of all of the above psychological quotients drawn together to enhance forecasting knowledge production.

5.1.1 Ethical risk intelligence practice: Although the expression 'EQ' is reserved for emotional intelligence within research literature, 'ethical intelligence' is perhaps a more pressing practical concern for our proposed risk radar use. In particular, what arguably matters most is a practical understanding of the ethical (and hence legal and reputational) *dos*

and *don'ts* of engaging with various primary or near-primary sources in order to elicit concrete risk information and gain contextual understanding. Conveniently, however, highly practical guidance on ethical codes for risk intelligence can be derived from codes of conduct developed by the competitive intelligence profession. Here the practical challenges arising with our boosted risk radar concept start to become very clear. The approach taken by the Strategic and Competitive Intelligence Professionals (SCIP) is to offer a succinct high-level code of conduct (SCIP, 1997). Some foundational ethical principles are discernible. Their guidance emphasises the importance of honesty within contexts of social interaction, the need for compliance with all laws, and the need to avoid or declare conflicts of interest. It also incorporates a more specific ethical imperatives covering adherence to company policies and guideline, and accurate disclosure of all relevant information when communicating with information sources. The effect of the code, then, is to accentuate the profession's specialisation in legitimate intelligence gathering capable of staving off reputationally damaging suggestions of deceit and subterfuge. In summary, we can conclude that organisations should focus effort towards clarifying and supporting the ethical and psychological 'risk intelligence' they decide they need, considering the above matters.

5.2 Meanings Two and Three: Risk intelligence processes and risk intelligent organisations

Throughout the discussion that follows, we selectively juxtapose some basic properties of the traditional risk management process with various similar organisational processes and related activities pertinent to the gathering and processing of intelligence. Our purpose will be to highlight opportunities for consolidation of similar and overlapping processes. This will enable us to outline a consolidated risk intelligence process, and by that token offer an outline vision of the risk intelligent organisation.

5.2.1 Learning from competitive, marketing and military intelligence processes: Maguire et al. (2009) and Ojiako et al. (2010, 2012) contend that competency to exploit novel situations has often eluded organisations. Furthermore, studies dealing with how businesses can learn from the military (Darling et al., 2005; Ojiako et al., 2010; Roche and Blaine, 2015) suggest that organisations, especially those competing in dynamic environments against irregular social threats from competitors, regulators, advocacy organisations, criminals, cyber-hackers and the like, can learn much from military approaches to combating irregular military threat. Seeking to contribute to this literature tradition by adding to the learning opportunities it has already proposed, we advocate that risk management is best developed in its risk intelligence process aspect through a practical focus on exploiting opportunities to consolidate and hybridise the traditional risk management process with conceptually similar marketing intelligence, competitive and military intelligence processes. There is no doubt from various organisational intelligence literatures (e.g. Dishman and Calof, 2008; Calof and Wright, 2008; McMullen et al. 2009) that various organisational intelligence processes can offer a range of information gathering and knowledge development enhancements. We will argue that organisational efforts to harness these competencies under the rubric of a general 'risk intelligence' process might best proceed from a constructively simple theoretical emphasis upon the challenge of boosting risk forecasting knowledge production for urgent and far-reaching engagement with irregular social threat.

5.2.2 Adopting the terminology of military intelligence processes: Emphasis on 'gathering' or 'collecting' information, which is key to competitive, marketing, business and other forms of intelligence practice within organisations (Taplin, 1989), has deep roots in decades of military intelligence theory and practice (Roche and Blaine, 2015). Military intelligence conceives of intelligence gathering as not just risky but also as sometimes requiring personal bravery and

sacrifice. A strong contrast arises here with the risk management concept of risk identification, whose sedentary connotations are (we think regrettably) consistent with much contemporary desk-based risk identification practice. An obvious yet curiously under-recognised benefit from importing military intelligence 'gathering' and 'collecting' metaphors invite is that they invite far more ambitious and energetic views regarding how organisations can develop attentiveness to social threat.

Some corresponding practical opportunity for hybridisation is therefore as follows. Whereas the ISO 31000 risk management process (ISO, 2009) begins with an *'establishing the context'* stage prior to its *'risk identification'* stage, US Military Joint Publication 2-0 (Department of Defense, 2013) moves through parallel '*planning and direction'* followed by *'collection'* stages. This document captures some of the logic of ISO 31000's first two stages in its view of *'planning and direction'* as being concerned with specifying what information is necessary for the successful achievement of specified military objectives, so that required *'collection'* activities can take place at the next stage. However, in the military intelligence process it is very clear that stage two intelligence '*collection'* conjoins logically with stage one '*direction'*. In the equivalent risk management process, such directed elicitation of active information gathering effort may not necessarily take place.

Perhaps, then, the ISO 310000 '*establishing the context'* stage is improvable through further provisions to establish contextual *uncertainties* whose purpose is very explicitly to focus intelligence gathering activities at stage two. The purpose of such new provisions might also be construed as 'pointing the risk radar in a particular direction' in terms of our primary guiding metaphor. Here we might also take into account our further layer of theoretical concern to focus risk intelligence effort on the conversion of unknown-unknowns, through further metaphorical conceptualisation of this enhanced and hybridised practice as serving to point the risk radar towards where the 'black swans' are most likely to fly in from. Arguably,

what makes this high level metaphorical view particularly valuable, then, is that it speaks directly to what might often be the practical necessity of establishing stage one specifications of contextual uncertainty which prime stage two information gathering to attune towards wholly novel social threats. Remembering that co-development of abstract and concrete risk knowledge is our risk intelligence goal, it is further worth mentioning that there is no reason why such priming could not specify stage two information-gathering challenges both in terms of demands placed on abstract theoretical imagination and on requirements for concrete risk information.

5.2.3 Learning from military intelligence practice: Risk analysis typically focuses on estimating probabilities and consequences for risks, so that risk evaluation can then consider each risk's significance with reference to pre-established criteria such as risk appetite or tolerance (Aven, 2012, 2017). The parallel practice within the military is to evaluate collected intelligence by ensuring its reliability and credibility through a process of filtering and weighting (Corkill, 2008; Wheaton, 2009). Such practice is espoused for example in the joint warfare publication on intelligence support published by the UK Ministry of Defence (2003).

If we are to re-envision risk management as a practice to be invigorated through active intelligence gathering, then we might regard simple reliability ratings for sources, and simple credibility ratings for the information or knowledge these sources provide, as providing a highly practical means to enhance consolidated risk intelligence processes dedicated to risk forecasting knowledge production. Notably, credibility judgments about risk forecasts must be differentiated from the probability judgments they help shape. To inquire into credibility is in part to question the appropriateness of some abstract theoretical framework which assembles information as knowledge, perhaps in simple 'story' form. Therefore, a risk intelligence process requirement to judge credibility, inspired by military intelligence

practice, can help sensitise those involved in risk forecasting knowledge production to the need to differentiate abstract from concrete risk knowledge in order to apply appropriate critical scrutiny to a risk forecast.

To reiterate our learning-from-the-military concerns, gaining an understanding of how military commanders have dealt with the dynamics of an ever-changing combat environment may include learning from relatively modern 'asymmetric' or 'unconventional' military approaches in response to combat experiences with irregular adversaries (see Kilcullen, 2010; Nagl, 2010; Ministry of Defence, 2010). The parallels with businesses needing to deal with cybersecurity and various other social threats are obvious. One important question arising is how risk management infrastructure can be refocused along more proactive 'boosted risk radar' lines towards deep and flexible engagement with irregular social threat sources. In practice terms, small, agile and highly cross-trained special risk intelligence teams or task forces (similar to military special operators) bolstered by competitive intelligence capability may create sufficient organisational capacity for grounding risk forecasting knowledge development in what Ojiako et al. (2010) call 'distributed intelligence'. This term refers to intelligence built from the lowest level of the organisation through widespread representation of its various functions in the special teams. This enables team members to contribute sufficiently broad and overlapping knowledge and experience pertaining to how social threat can impact organisations. In military circles, every special operator is deemed mandated to gather intelligence. In organisations, every employee across the entire spectrum of the organisation can similarly, at the very least, be seen as a proactive gatherer of intelligence who can interact with the special teams. This suggestion is intended to gel with commonplace ERM philosophy emphasising universal responsibility for initiating risk communications throughout the corporate nervous system (Institute of Risk Management, 2011).

Organisations can also develop risk forecasting knowledge through risk simulations structured in accordance with military '*red teaming'* practice (Zenko, 2015). This can entail realistic role-play rehearsal of attacks upon organisations, in order to enrich forecasts, identify security vulnerabilities and improve planning protocols. Dedicated 'red teams' can also offer decision support. Well-known (2013) UK Ministry of Defence guidance explaining how is partly of interest for its surprising use of business terminology. It defines red teaming as "the independent application of a range of structures, creative and critical thinking techniques to assist the end user make a better informed decision to produce a more robust product" (p.4). Lauder (2009) observes that '*red teaming'* in this sense usually entails voicing contrarian positions to inculcate more open-minded group decision-making, either in scenario exercises or in real life decision-making contexts. We can summarise its contribution to risk forecasting practice as one that also creates opportunities for the application of critical scrutiny to the co-production of abstract and concrete forecasting knowledge.

6.0 Conclusion

The paper has advocated for enhancement of risk forecasting practice under the influence of the multi-layered terminology and theory drawn together. Our theories pertaining to critical application of Rumsfeld's knowledge quadrants for co-development of abstract and concrete forecasting knowledge, to the boosted risk radar, and to risk intelligence considered in the three interrelated aspects we propose, all offer novelty. By relating these theories both to one another and to highly practical proposals for enhancing organisational risk forecasting, we assure the novelty of our contribution to risk management and forecasting literatures, particularly in relation to challenges created by irregular social threat in general and cybersecurity in particular.

Thus, we have provided initial terminological and conceptual groundwork for theory development and for improvements to forecasting practice. Further research on risk forecasting as critical knowledge production focused on Rumsfeld's binary knowledge ontology and its four quadrants, is called for. Psychometric research may assist if it can supply measurement tools showing that practitioners can estimate separate levels of abstract and concrete forecasting knowledge. If it can also be proven that this knowledge ontology is helpful for critical scrutiny purposes, then the case for improving risk management as we advocate will strengthen.

References

Aabo, T., Fraser, J., & Simkins, B. (2005). The rise and evolution of the chief risk officer: enterprise risk management at Hydro One. *Journal of Applied Corporate Finance*, 17(3), 62-75.

Ackermann, F., Eden, C., Williams, T., & Howick, S. (2007). Systemic risk assessment: a case study. *Journal of the Operational Research Society*, 58(1), 39-51.

Alfieri, A. (2005). The fall of legal ethics and the rise of risk management. *Georgia Law Journal*, 94, 1909 - 1956.

Althaus, C. (2005). A disciplinary perspective on the epistemological status of risk. *Risk Analysis*, 25(3), 567-588.

Ansoff, H. (1975). Managing strategic surprise by response to weak signals. *California Management Review*, 18(2), 21-33.

Árvai, J. (2014). The end of risk communication as we know it. *Journal of Risk Research*, 17(10), 1245-1249.

Aven, T., 2012. Foundational issues in risk assessment and risk management. Risk Analysis, 32(10), 1647-1656.

Aven, T., 2017. An Emerging New Risk Analysis Science: Foundations and Implications. *Risk Analysis*, DOI: https://doi.org/10.1111/risa.12899 (In Press).

Aven, E., & Aven, T. (2015). On the need for rethinking current practice that highlights goal achievement risk in an enterprise context. *Risk Analysis*, 35(9), 1706-1716.

Balogun, J., Gleadle, P., Hailey, V., & Willmott, H. (2005). Managing Change Across Boundaries: Boundary‐Shaking Practices. *British Journal of Management*, 16(4), 261-278.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17 (1), 99-120

Biscaro, C., & Comacchio, A. (2017). Knowledge Creation Across Worldviews: How Metaphors Impact and Orient Group Creativity. *Organization Science*, 29 (1), 58-79.

Brännmark, J., & Sahlin, N. (2010). Ethical theory and the philosophy of risk: first thoughts. *Journal of Risk Research*, 13(2), 149-161.

Braunscheidel, M., & Suresh, N. (2009). The organisational antecedents of a firm's supply chain agility for risk mitigation and response. *Journal of Operations Management*, 27(2), 119-140.

Brislin, R., Worthley, R., & Macnab, B. (2006). Cultural intelligence: Understanding behaviours that serve people's goals. *Group & Organisation Management*, 31(1), 40-55.

British Standards Institution. (2014). *BS 65000 Guidance on Organisational Resilience*. Available at: http://www.standardsuk.com/, accessed 25/03/18.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning*, 48(4), 265-276.

Calof, J., & Wright, S. (2008). Competitive intelligence: A practitioner, academic and inter-disciplinary perspective. *European Journal of Marketing*, 42(7/8), 717-730.

Campbell, S. (2006). Risk and the Subjectivity of Preference. *Journal of Risk Research*, 9(03), 225-242.

Chen, M., & Miller, D. (1994). Competitive attack, retaliation and performance: an expectancy ‐ valence framework. *Strategic Management Journal*, 15(2), 85-102.

Chipulu, M., Ojiako, U. and Marshall, A., 2016. Consumer action in response to ethical violations by service operations firms: The impact of heterogeneity. *Society and Business Review*, 11(1), 24-45.

Christoffersen, M. (2017). Risk, danger, and trust: refining the relational theory of risk. *Journal of Risk Research*, DOI: https://doi.org/10.1080/13669877.2017.1301538 (In Press).

CNN. (2016). *RUMSFELD / KNOWNS*. [online video] Available at: https://www.youtube.com/watch?v=REWeBzGuzCc, accessed 02/04/18.

Corkill, J. (2008). Evaluation a critical point on the path to intelligence. *Journal of the Australian Institute of Professional Intelligence Officers*, 16(1), 3-11.

Cornelissen, J. (2005). Beyond compare: Metaphor in organisation theory. *Academy of Management Review*, 30(4), 751-764.

Cornelissen, J., Kafouros, M., & Lock, A. (2005). Metaphorical images of organisation: How organisational researchers develop and select organisational metaphors. *Human Relations*, 58(12), 1545-1578.

Committee of Sponsoring Organisations of the Treadway Commission (COSO). (2017). *Enterprise Risk Management: integrating with strategy and performance.* http://www.standardsuk.com, accessed 28/03/18.

Crant, J. (2000). Proactive behaviour in organisations. *Journal of Management*, 26(3), 435-462.

Crutch, S., Connell, S., & Warrington, E. (2009). The Different Representational Frameworks Underpinning Abstract and Concrete Knowledge: evidence from odd-one-out judgements. *Quarterly Journal of Experimental Psychology*, 62 (7) 1377-1390.

Dagdeviren, H., Lund-Thomsen, P. and McCann, L. (2017). Multiple paths through the complexities of globalization: The next three years of Competition & Change. *Competition & Change*, 21(1), 3–9.

Darling, M., Parry, C., & Moore, J. (2005). Learning in the thick of it. *Harvard Business Review*, 83(7), 84-93.

Daudigeos, T. (2013). In their profession's service: how staff professionals exert influence in their organisation. *Journal of Management Studies*, 50(5), 722-749.

Daunt, K., & Harris, L. (2012). Exploring the forms of dysfunctional customer behaviour: A study of differences in servicescape and customer disaffection with service. *Journal of Marketing Management*, 28(1-2), 129-153.

Department of Defense. (2013). *JP 2-0: Joint Intelligence*. http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf, accessed 26/12/17.

Dickinson, G. (2001). Enterprise risk management: Its origins and conceptual foundation. Geneva Papers on Risk and Insurance. *Issues and Practice*, 26(3), 360-366.

Dindar, S., Kaewunruen, S., & An, M. (2016). Identification of appropriate risk analysis techniques for railway turnout systems. *Journal of Risk Research*, DOI: 10.1080/13669877.2016.1264452 (In Press).

Dishman, P., & Calof, J. (2008). Competitive intelligence: a multiphasic precedent to marketing strategy. *European Journal of Marketing*, 42(7/8), 766-785.

Donnelly-Saalfield, J. (2009). Irreparable Harms: How the Devastating Effects of Oil Extraction in Nigeria Have Not Been Remedied by Nigerian Courts, the African Commission, or US Courts. *Hastings West-Northwest Journal of Environmental Law and Policy*, 15, 371-420.

Dussauge, P., Garrette, B., & Mitchell, W. (2000). Learning from competing partners: outcomes and durations of scale and link alliances in Europe, North America and Asia. *Strategic Management Journal*, 21 (2), 99-126.

Elenkov, D. (1997). Strategic uncertainty and environmental scanning: The case for institutional influences on scanning behaviour. *Strategic Management Journal*, 18 (4), 287-302.

Elster, J. (1989). *Nuts and Bolts for the Social Sciences*. Cambridge University Press.

Evans, D. (2012). *Risk Intelligence: How to Live with Uncertainty*. New York: Free Press.

EY (2014). *Third-party risk management: EY Integrity Diligence*. Pub. Ernst & Young.

Fisk, R., Grove, S., Harris, L., Keeffe, D., Daunt, K., Russell-Bennett, R., & Wirtz, J. (2010). Customers behaving badly: a state of the art review, research agenda and implications for practitioners. *Journal of Services Marketing*, 24(6), 417-429.

Foss, K., & Rodgers, W. (2011). Enhancing information usefulness by line managers' involvement in cross-unit activities. *Organisation Studies*, 32(5), 683-703.

Francis, R., & Armstrong, A. (2003). Ethics as a risk management strategy: The Australian experience. *Journal of Business Ethics*, 45(4), 375-385.

Franken, A., Goffin, K., Szwejczewski, M., & Kutsch, E. (2014). *Roads to Resilience: Building Dynamic Approaches to Risk*. Pub. Cranfield Management School.

Freeman, O. (1999). Competitor intelligence: information or intelligence?. *Business Information Review*, 16(2), 71-77.

Frey, M., & Detterman, D. (2004). Scholastic assessment or g? The relationship between the scholastic assessment test and general cognitive ability. *Psychological Science*, 15(6), 373-378.

Giachetti, C., Lampel, J., & Pira, S. (2017). Red queen competitive imitation in the UK mobile phone industry. *Academy of Management Journal*, 60(5), 1882-1914.

Gottfredson, L. (1997). Mainstream Science on Intelligence (editorial), *Intelligence*. 24, 13–23.

Grégoire, Y., & Fisher, R. (2008). Customer betrayal and retaliation: when your best customers become your worst enemies. *Journal of the Academy of Marketing Science*, 36(2), 247-261.

Grégoire, Y., Tripp, T., & Legoux, R. (2009). When customer love turns into lasting hate: The effects of relationship strength and time on customer revenge and avoidance. *Journal of Marketing*, 73(6), 18-32.

Hambrick, D. (1981). Specialization of environmental scanning activities among upper level executives. *Journal of Management Studies*, 18(3), 299-320.

Hansson, S. (2004). Fallacies of risk. *Journal of Risk Research*, 7(3), 353-360.

Harrison G. and Phillips R. (2014). *Subjective Beliefs and Statistical Forecasts of Financial Risks: The Chief Risk Officer Project*. In: Andersen T.J. (eds) Contemporary Challenges in Risk Management. Palgrave Macmillan, London.

Holmqvist, M. (2003). A dynamic model of intra-and interorganisational learning. *Organisation Studies*, 24(1), 95-123.

Hoyt, R., & Liebenberg, A. (2011). The value of enterprise risk management. *Journal of Risk and Insurance*, 78(4), 795-822.

Huang, C., Wu, T., & Renn, O. (2016). A Risk Radar driven by Internet of intelligences serving for emergency management in community. *Environmental Research*, 148, 550-559.

Huurne, E., & Gutteling, J., 2008. Information needs and risk perception as predictors of risk information seeking. *Journal of Risk Research*, 11(7), 847-862.

Ifedi, J., & Anyu, J. (2011). Blood Oil," Ethnicity, and Conflict in the Niger Delta Region of Nigeria. *Mediterranean Quarterly*, 22(1), 74-92.

Institute of Risk Management. (2011). *Risk Appetite and Tolerance: a guidance paper from the Institute of Risk Management*. Pub. Institute of Risk Management.

Ireland, R., Hitt, M., & Vaidyanath, D. (2002). Alliance management as a source of competitive advantage. *Journal of Management*, 28(3), 413-446.

ISO (2009). *ISO 31000: Risk Management - Principles and Guidelines*. Geneva: International Standards Organisation.

Jaworski, B., & Kohli, A. (1993). Market Orientation: antecedents and consequences. *Journal of Marketing*, 57, 53-70

Jovanovic, A. (2012). *From iNTeg-Risk to European Emerging Risk Radar (E2R2), Managing Early Warnings - what and how to look for?*, Book of Abstracts of 4th iNTeg-Risk Conference 2012, p. 46.

Jovanovic, A., Balos, D., & Yan, L. (2012). The European Emerging Risk Radar Initiative–a Chance for China?. International Symposium on Safety Science and Engineering in China, 2012 (ISSSE-2012), *Procedia Engineering*, 43, 489-493.

Jovanović, A., & Baloš, D. (2013). iNTeg-Risk project: concept and first results. *Journal of Risk Research*, 16(3-4), 275-291.

Karanja, E., & Rosso, M. (2017). The Chief Risk Officer: a study of roles and responsibilities. *Risk Management*, 19(2), 103-130.

Kaspersky (2014). *Unveiling "Careto" – The Masked APT. Kaspersky Lab*, https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf, accessed 11/03/18.

Kavusan, K., Noorderhaven, N., & Duysters, G. (2016). Knowledge acquisition and complementary specialization in alliances: The impact of technological overlap and alliance experience. *Research Policy*, 45(10), 2153-2165.

Kilcullen, D. (2010). *Counterinsurgency*. Pub. London: Hurst.

Korsgaard, M., Brower, H., & Lester, S. (2015). It isn't always mutual: A critical review of dyadic trust. *Journal of Management*, 41(1), 47-70.

Kramer, R. (2008). *Organizational Paranoia: origins and dysfunctional consequences of exaggerated distrust and suspicion in the workplace*. In 21st Century Handbook of Organizations: a reference handbook. C. Wankel (ed.). Los Angeles: Sage Publications, 231-238

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy*, 9(3), 49-51.

Lauder, M. (2009). Red dawn: The emergence of a red teaming capability in the Canadian forces. *Canadian Army Journal*, 12(2), 25-36.

Leva, M., Balfe, N., McAleer, B., & Rocke, M. (2017). Risk registers: structuring data collection to develop risk intelligence. *Safety Science*, 100 (Part B), 143-156.

Lidskog, R. and Sjödin, D. (2016). Risk governance through professional expertise. Forestry consultants' handling of uncertainties after a storm disaster. *Journal of Risk Research*, 19(10), 1275-1290.

Lieberman, M., & Asaba, S. (2006). Why do firms imitate each other?. *Academy of Management Review*, 31(2), 366-385.

Lin, L., Rivera, C., Abrahamsson, M., & Tehler, H. (2017). Communicating risk in disaster risk management systems–experimental evidence of the perceived usefulness of risk descriptions. *Journal of Risk Research*, 20(12), 1534-1553.

Lindaas, O., & Pettersen, K. (2016). Risk analysis and Black Swans: two strategies for de-blackening. *Journal of Risk Research*, 19(10), 1231-1245.

Logan, D. (2009). Known Knowns, Known Unknowns, Unknown Unknowns and the Propagation of Scientific Enquiry. *Journal of Experimental Botany*, 60(3) 712–714.

Lyng, S. (ed). (2005). *Edgework. The Sociology of Risk-taking*. New York: Routledge.

Maguire, S., Ojiako, U., & Robson, I. (2009). The intelligence alchemy and the twenty‐first century organisation. *Strategic Change*, 18(3‐4), 125-139.

Månsson, P., Abrahamsson, M., & Tehler, H. (2017). Aggregated risk: an experimental study on combining different ways of presenting risk information. *Journal of Risk Research*, DOI: https://doi.org/10.1080/13669877.2017.1391315 (In Press).

Marshall, R., Telofski, R., Ojiako, U., & Chipulu, M. (2012). An Examination of 'Irregular Competition' between Corporations and NGOs. *Voluntas*, 23, 371-391.

Marshall, A., & Ojiako, U. (2013). Managing Risk through the Veil of Ignorance. *Journal of Risk Research*, 16 (10), 1225-1239.

Marshall, A., & Ojiako, U. (2015). A realist philosophical understanding of entrepreneurial risk-taking. *Society and Business Review*, 10 (2), 178-193.

Marshall, A., Bashir, H., Ojiako, U., & Chipulu, M. (2018). A Machiavellian behavioural framing of social conflict risks in supply chains" *Management Research Review*, DOI: 10.1108/MRR-01-2018-0022 (In Press).

Marshall, A., Ojiako, U., & Chipulu, M. (2019). Risk Appetite: A Futility, Perversity and Jeopardy critique of over-optimistic Corporate Risk Taking" *International Journal of Organisational Analysis*, In Press.

McDonald, M., Smith, B., & Ward, K. (2006). *Marketing due diligence: reconnecting strategy to share price*. Butterworth-Heinemann.

McMullen, J., Shepherd, D., & Patzelt, H. (2009). Managerial (in) attention to competitive threats. *Journal of Management Studies*, 46(2), 157-181.

Mellers, B., Stone, E., Atanasov, P., Rohrbaugh, N., Metz, S., Ungar, L., Bishop, M., Horowitz, M., Merkle, E., & Tetlock, P. (2015). The psychology of intelligence analysis: Drivers of prediction accuracy in world politics. *Journal of Experimental Psychology: Applied*, 21(1):1-14.

Merkelsen, H. (2011). Institutionalized ignorance as a precondition for rational risk expertise. *Risk Analysis*, 31(7), 1083-1094.

Ministry of Defence (UK) (2003). *Joint Warfare Publication 2-00: Intelligence Support to Joint Operations*. Joint Doctrine and Concepts Centre, Pub. Ministry of Defence.

Ministry of Defence (UK) (2010). *Countering insurgency: Army Field Manual, Vol. 1 Pt. 10 (AC71876)*, Pub. Ministry of Defence.

Ministry of Defence (UK) (2013). *Red Teaming Guide*, *Development, Concepts and Doctrine Centre*. 2nd Edition, Pub. Ministry of Defence.

Montgomery, K., & Oliver, A. (2007). A fresh look at how professions take shape: Dual-directed networking dynamics and social boundaries. *Organisation Studies*, 28(5), 661-687.

Moosa, I. (2007). Misconceptions about operational risk. *Journal of Operational Risk*, 1(4), 97-104.

Morgan, G. (2006). *Images of Organization*. Sage Publications.

Muzio, D., Brock, D., & Suddaby, R. (2013). Professions and institutional change: Towards an institutionalist sociology of the professions. *Journal of Management Studies*, 50(5), 699-721.

Nagl, J. (2010). Thinking globally, acting locally: counterinsurgency lessons from modern wars. *Journal of Strategic Studies*, 33(1) 2010, 16-59

Nelson, R. (1991). Why do firms differ, and how does it matter?. *Strategic Management Journal*, 12(S2), 61-74.

Nepomuceno, M., Rohani, M., & Grégoire, Y. (2017). *Consumer Resistance: From Anti-Consumption to Revenge. In Consumer Perception of Product Risks and Benefits*. Springer International Publishing, pp. 345-364.

Nicolini, D., Gherardi, S. & Yanow, D. 2016. *Introduction: toward a practice-based view of knowing and learning in organizations*. In "Knowing in Organizations" D. Nicolini, Gherardi, S & Yanow, D. (eds). Routledge. Chapter 1.

Nuki, P. & Shaikh, A. (2018). *Scientists Put on Alert for Deadly New Pathogen: 'Disease X'*. The Telegraph Online 10th March 2018 edition, https://www.telegraph.co.uk/news/2018/03/09/world-health-organization-issues-alert-disease-x/, accessed 24/04/18.

Ojiako, U., Johnson, J., Chipulu, M., & Marshall, A. (2010). Unconventional competition – drawing lessons from the military. *Prometheus*, 28(4), 327-342.

Ojiako, U., Marshall, A., Luke, M., & Chipulu, M. (2012). Managing competition risk: A critical realist philosophical exploration. *Competition & Change*, 16(2), 130-149.

Orlikowski, W. (2002). Knowing in Practice: Enacting a Collective Capability in Distributed Organizing. *Organization Science*, 13(3), 249–273.

Parker, S., Bindl, U., & Strauss, K. (2010). Making things happen: A model of proactive motivation. *Journal of Management*, 36(4), 827-856.

Pernell, K., Jung, J., & Dobbin, F. (2017). The Hazards of Expert Control: Chief Risk Officers and Risky Derivatives. *American Sociological Review*, 82(3), 511-541.

Power, M. (2004). The risk management of everything. *Journal of Risk Finance*, 5(3), 58-65.

Power, M. (2009). The risk management of nothing. *Accounting, Organisations and Society*, 34(6), 849-855.

Power, M., Scheytt, T., Soin, K., & Sahlin, K. (2009). Reputational risk as a logic of organising in late modernity. *Organisation Studies*, 30(2-3), 301-324.

PWC (2013). *TPRM Viewpoint: PwC Viewpoint on Third Party Risk Management*. Pub. PricewaterhouseCoopers.

Mayer, J., Salovey, P., & Caruso, D. (2004). Emotional intelligence: Theory, findings, and implications. *Psychological Inquiry*, 15, 197-215.

Pawson, R., Wong, G., & Owen, L. (2011). Known Knowns, Known Unknowns, Unknown Unknowns: the predicament of evidence-based policy. *American Journal of Evaluation*, 32(4), 518-546.

Rifkin, J. (2001). *Age of Access: the new culture of hypercapitalism, where all of life is a paid-for experience*. Pub. Jeremy P. Tarcher.

Roche, E., & Blaine, M. (2015). The intelligence gap: What the multinational enterprise can learn from government and military intelligence organisations. *Thunderbird International Business Review*, 57(1), 3-13.

Rowley, J. (2007). The Wisdom Hierarchy: representations of the DIKW hierarchy. *Journal of Information and Communication Science*, 33(2), 163-180.

Sahi S. (2017). A Study of WannaCry Ransomware Attack. *International Journal of Engineering Research in Computer Science and Engineering*, 4(9), 5-7.

Schiller, F., & Prpich, G. (2014). Learning to organise risk management in organisations: what future for enterprise risk management?. *Journal of Risk Research*, 17(8), 999-1017.

Schoemaker, P., Day, G., & Snyder, S. (2013). Integrating Organizational Networks, Weak Signals, Strategic Radars and Scenario Planning. *Technological Forecasting and Change*, 80(4), 815-824.

Schminke, M., Caldwell, J., Ambrose, M., & McMahon, S. (2014), Better than ever? Employee reactions to ethical failures in organisations, and the ethical recovery paradox. *Organisational Behaviour and Human Decision Processes*, 123 (2), 206-219.

Scott, W. (2003). *Organizations: Rational, Natural, and Open systems*. Prentice Hall, Upper Saddle River, New Jersey, fifth edition,

SCIP (1997). *Competitive Intelligence Ethics: Navigating the Gray Zone*. Pub. Strategic and Competitive Intelligence Professionals.

Sison, A. (2000). Integrated risk management and global business ethics. *Business Ethics: A European Review*, 9(4), 288-295.

Sitkin, S., & Pablo, A. (1992). Reconceptualizing the determinants of risk behaviour. *Academy of Management Review*, 17(1), 9-38.

Slonim, O. (2017). National intelligence: A tool for political forecasting and the forecasting of rare events. *Technological Forecasting and Social Change*, DOI: https://doi.org/10.1016/j.techfore.2017.04.019 (In Press).

Smith, B., & Raspin, P. (2011). *Creating market insight: How firms create value from market understanding*. John Wiley & Sons.

Smith, R., & Lindsay, D. (2012). From information to intelligence management. *Business Information Review*, 29(2), 121-124.

Smyth, V. (2017). Software vulnerability management: how intelligence helps reduce the risk. *Network Security*, 2017(3), 10-12.

Spira, L., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. Accounting, *Auditing & Accountability Journal*, 16(4), 640-661.

Stanovich, K. (2009a). *What intelligence tests miss: The psychology of rational thought*. New Haven, CT: Yale University Press.

Stanovich, K. (2009b). Rational and irrational thought: The thinking that IQ tests miss. *Scientific American Mind*, 20(6), 34-39.

Stanovich, K., & West, R. (2009). What intelligence tests miss. *The Psychologist*, 27 (2), 80-83.

Suddaby, R., & Viale, T. (2011). Professionals and field-level change: Institutional work and the professional project. *Current Sociology*, 59(4), 423-442.

Taplin, W. (1989). Six general principles of intelligence. *International Journal of Intelligence and Counter Intelligence*, 3(4), 475–491.

Thompson, P. (1986). The philosophical foundations of risk. *The Southern Journal of Philosophy*, 24(2), 273-286.

Thompson, K., & Bloom, D., 2000. Communication of risk assessment information to risk managers. *Journal of Risk Research*, 3(4), 333-352

Tsoukas, H. (2009). A Dialogical Approach to the Creation of New Knowledge in Organizations. *Organization Science*, 20(6), 941–957.

Vallacher, R., & Wegner, D. (1985). *A Theory of Action Identification*. Lawrence Erlbaum Associates, Hillsdale NJ.

Valverde, L. (1991). Cognitive Status of Risk: A Response to Thompson. RISK: Health, Safety & Environment, 2 (4), p.313-339.

Virvilis, N. and Gritzalis, D. (2013). *The Big Four – What We Did Wrong in Advanced Persistent Threat Detection?* International Conference on Availability, Reliability and Security. 2-6 Sept. 2013.

Ward, J. and Ostrom, A. (2006). Complaining to the masses: The role of protest framing in customer-created complaint web sites. *Journal of Consumer Research*, 33(2), 220-230.

Weick, K., & Sutcliffe, K. (2001). *Managing the Unexpected: resilient performance in an age of uncertainty*. John Wiley & Sons.

Weick, K., & Putnam, T. (2006). Organizing for Mindfulness: eastern wisdom and western knowledge. *Journal of Management Inquiry*, 15(3), 275-287.

Werhane P (1999). *Moral Imagination and Management Decision-Making*. Oxford University Press.

Wheaton, K. (2009). Evaluating intelligence: answering questions asked and not. *International Journal of Intelligence and Counterintelligence*, 22(4), 614-631.

Wright, S., & Calof, J. (2006). The quest for competitive, business and marketing intelligence: A country comparison of current practices. *European Journal of Marketing*, 40(5/6), 453-465.

Wu, D., Chen, S., & Olson, D. (2014). Business intelligence in risk management: Some recent progresses. *Information Sciences*, 256, 1-7.

Zenko, M. (2015). *Red Team: How to succeed by thinking like the enemy*. Pub. Basic Books.

Zinn, J. (2017). The meaning of risk-taking–key concepts and dimensions. *Journal of Risk Research*, DOI: 10.1080/13669877.2017.1351465 (In Press).

Zizekian Studies. (2015). Slavoj Zizek | Unknown Knowns and Psychoanalysis [online video], https://www.youtube.com/watch?v=i1IjkfcwoHs, accessed 02/04/18.

Zourrig, H., Chebat, J., & Toffoli, R. (2009). Consumer revenge behaviour: a cross-cultural perspective. *Journal of Business Research*, 62(10), 995-1001